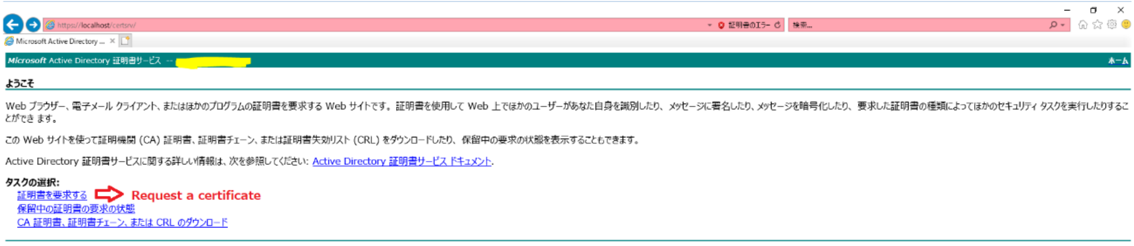
1. AD Sever Side:

- AD server - 【Request the certificate】



Microsoft Active Directory 証明書サービス -- [redacted]

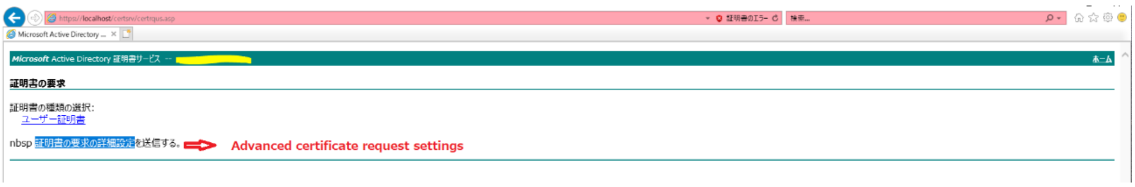
ようこそ

Web ブラウザー、電子メール クライアント、またはほかのプログラムの証明書を要求する Web サイトです。証明書を使用して Web 上でほかのユーザーがあなた自身を識別したり、メッセージに署名したり、メッセージを暗号化したり、要求した証明書の種類によってほかのセキュリティ タスクを実行したりすることができ ます。

この Web サイトを使って証明機関 (CA) 証明書、証明書チェーン、または証明書失効リスト (CRL) をダウンロードしたり、保留中の要求の状態を表示することもできます。

Active Directory 証明書サービスに関する詳しい情報は、次を参照してください: Active Directory 証明書サービス ドキュメント.

タスクの選択:
証明書を要求する ⇨ Request a certificate
保留中の証明書の要求の状態
CA 証明書、証明書チェーン、または CRL のダウンロード

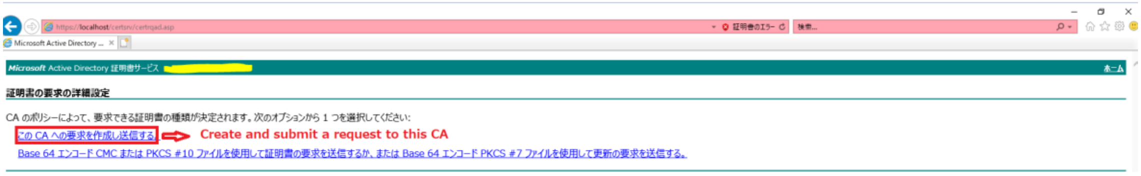

https://localhost/certsrv/certrqus.asp
証明書のエラー
検索...
Microsoft Active Directory ...
ホーム

Microsoft Active Directory 証明書サービス -- [redacted]

証明書の要求

証明書の種類の選択:
ユーザー証明書

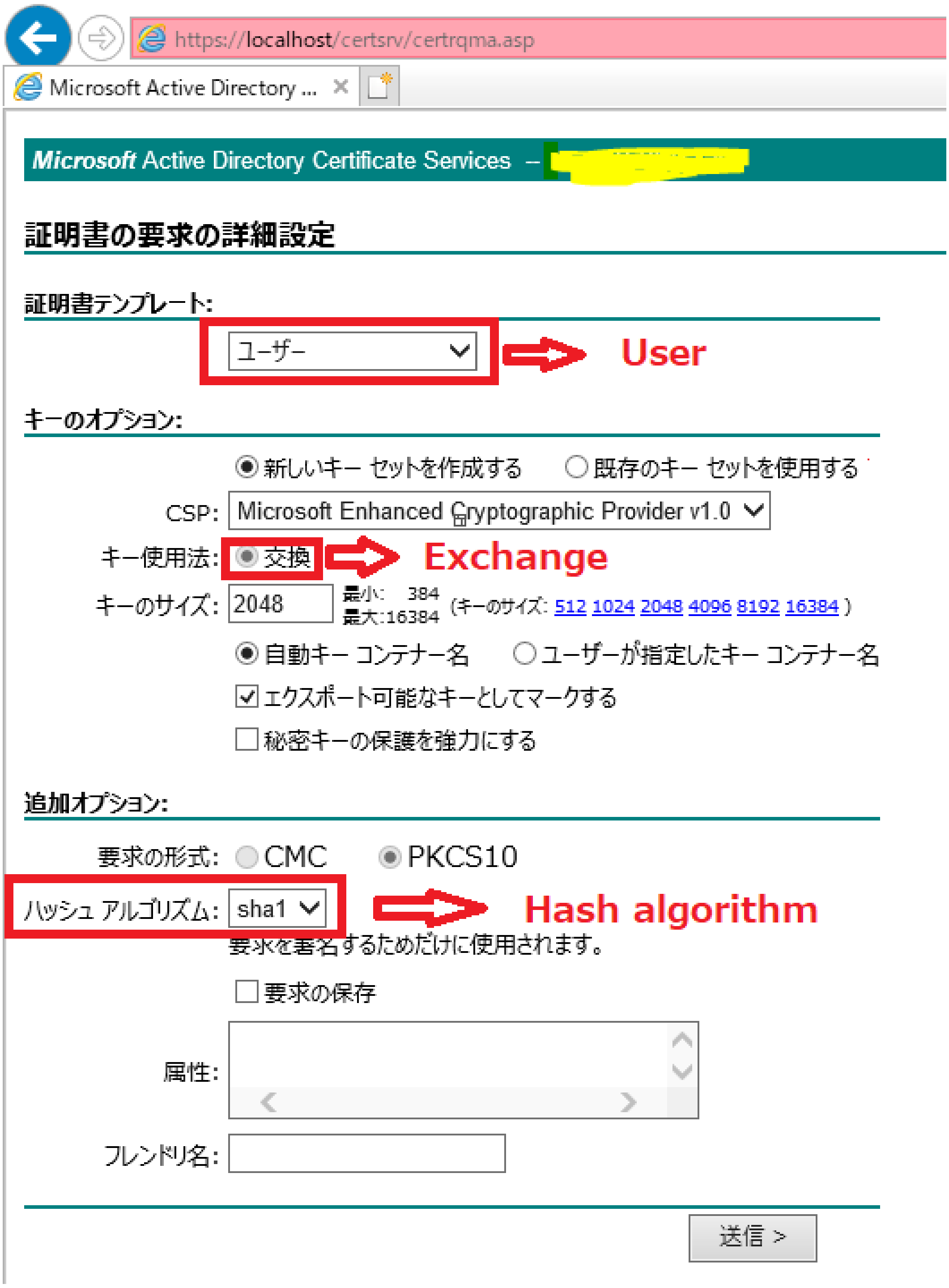
nbsp 証明書の要求の詳細設定を送信する。 ⇨ Advanced certificate request settings


https://localhost/certsrv/certrqad.asp
証明書のエラー
検索...
Microsoft Active Directory ...
ホーム

Microsoft Active Directory 証明書サービス [redacted]

証明書の要求の詳細設定

CA のポリシーによって、要求できる証明書の種類が決定されます。次のオプションから 1 つを選択してください:
この CA への要求を作成し送信する。 ⇨ Create and submit a request to this CA
Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する。



https://localhost/certsrv/certrqma.asp

Microsoft Active Directory ...

Microsoft Active Directory Certificate Services – [redacted]

証明書の要求の詳細設定

証明書テンプレート:

ユーザー

User

キーのオプション:

● 新しいキー セットを作成する ○ 既存のキー セットを使用する

CSP: Microsoft Enhanced Cryptographic Provider v1.0

キー使用法: ● 交換

Exchange

キーのサイズ: 2048 最小: 384 最大:16384 (キーのサイズ: 512 1024 2048 4096 8192 16384)

● 自動キー コンテナー名 ○ ユーザーが指定したキー コンテナー名

☑ エクスポート可能なキーとしてマークする

□ 秘密キーの保護を強力にする

追加オプション:

要求の形式: ○ CMC ● PKCS10

ハッシュ アルゴリズム: sha1

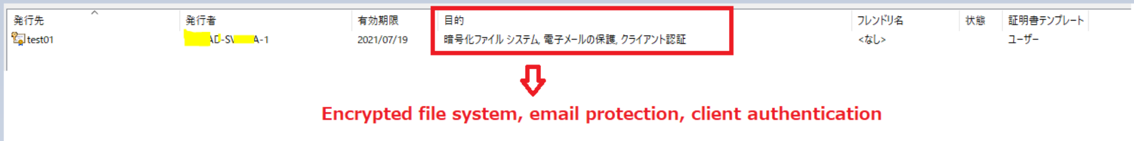
Hash algorithm

要求を署名するためだけに使用されます。

□ 要求の保存

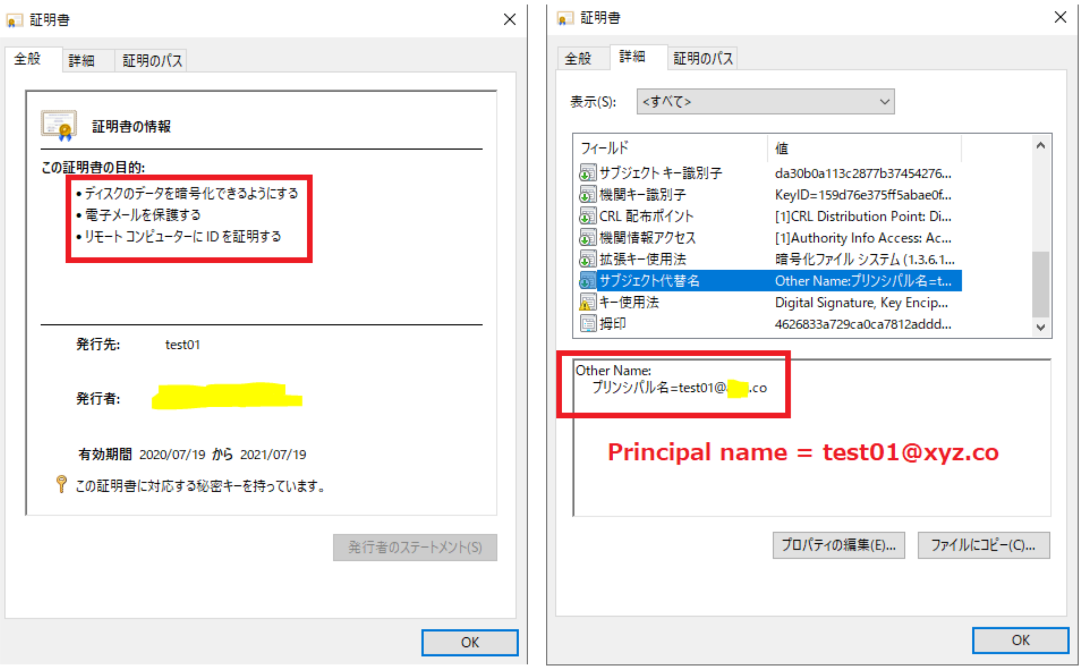
属性:

フレンドリ名:



発行先	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプレート
test01	[redacted]AD-SV[redacted]A-1	2021/07/19	暗号化ファイル システム, 電子メールの保護, クライアント認証	<なし>		ユーザー

Encrypted file system, email protection, client authentication



証明書の情報

この証明書の目的:

- ディスクのデータを暗号化できるようにする
- 電子メールを保護する
- リモート コンピューターに ID を証明する

発行先: test01

発行者: [redacted]

有効期間 2020/07/19 から 2021/07/19

この証明書に対応する秘密キーを持っています。

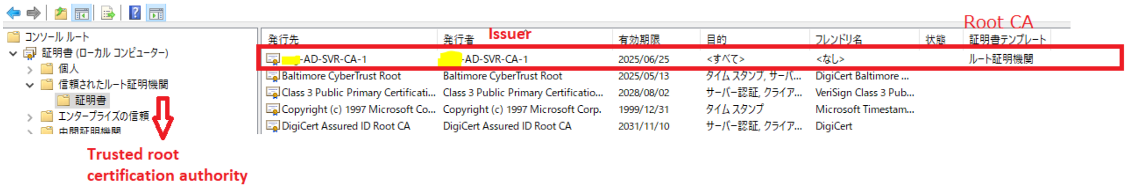
表示(S): <すべて>

フィールド	値
サブジェクト キー識別子	da30b0a113c2877b37454276...
機関キー識別子	KeyID=159d76e375ff5abae0f...
CRL 配布ポイント	[1]CRL Distribution Point: Di...
機関情報アクセス	[1]Authority Info Access: Ac...
拡張キー使用法	暗号化ファイル システム (1.3.6.1...
サブジェクト代替名	Other Name:プリンシパル名=t...
キー使用法	Digital Signature, Key Encip...
拇印	4626833a729ca0ca7812addd...

Other Name:
プリンシパル名=test01@[redacted].co

Principal name = test01@xyz.co

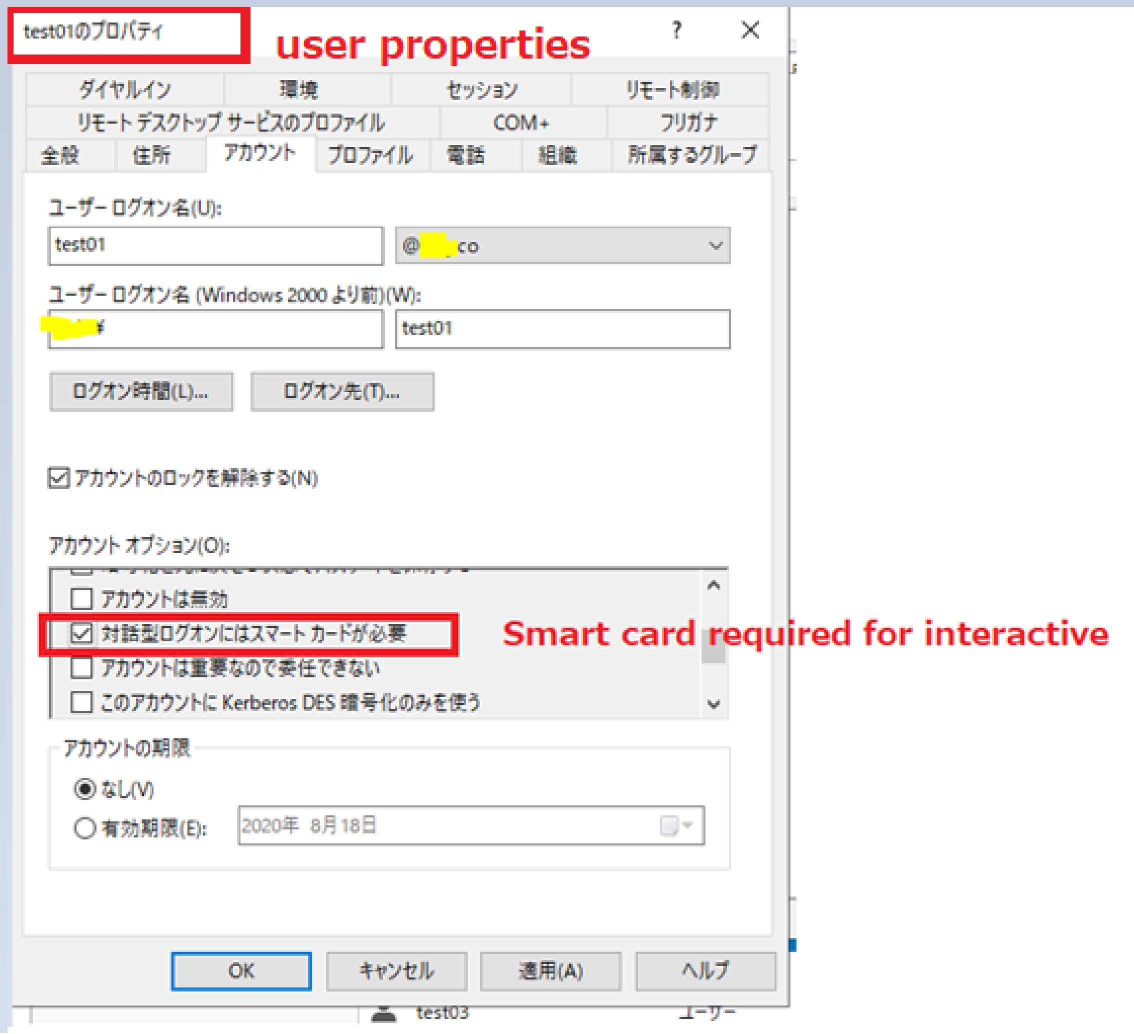
The UPN of the user as subject alternative name.



発行先	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプレート
[redacted]-AD-SVR-CA-1	[redacted]-AD-SVR-CA-1	2025/06/25	<すべて>	<なし>		ルート証明機関
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/05/13	タイム スタンプ, サーバ...	DigiCert Baltimore ...		
Class 3 Public Primary Certificati...	Class 3 Public Primary Certificatio...	2028/08/02	サーバー認証, クライア...	VeriSign Class 3 Pub...		
Copyright (c) 1997 Microsoft Co...	Copyright (c) 1997 Microsoft Corp.	1999/12/31	タイム スタンプ	Microsoft Timestam...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	サーバー認証, クライア...	DigiCert		

Check DC (domain controller) to trust certificate (the issuer in the list of trusted root CAs)

- AD server - 【User Setting】



test01のプロパティ

user properties

ユーザー ログオン名(U):

test01 @[redacted].co

ユーザー ログオン名 (Windows 2000 より前)(W):

[redacted]¥ test01

☑ アカウントのロックを解除する(N)

アカウント オプション(O):

□ アカウントは無効

☑ 対話型ログオンにはスマート カードが必要

□ アカウントは重要なので委任できない

□ このアカウントに Kerberos DES 暗号化のみを使う

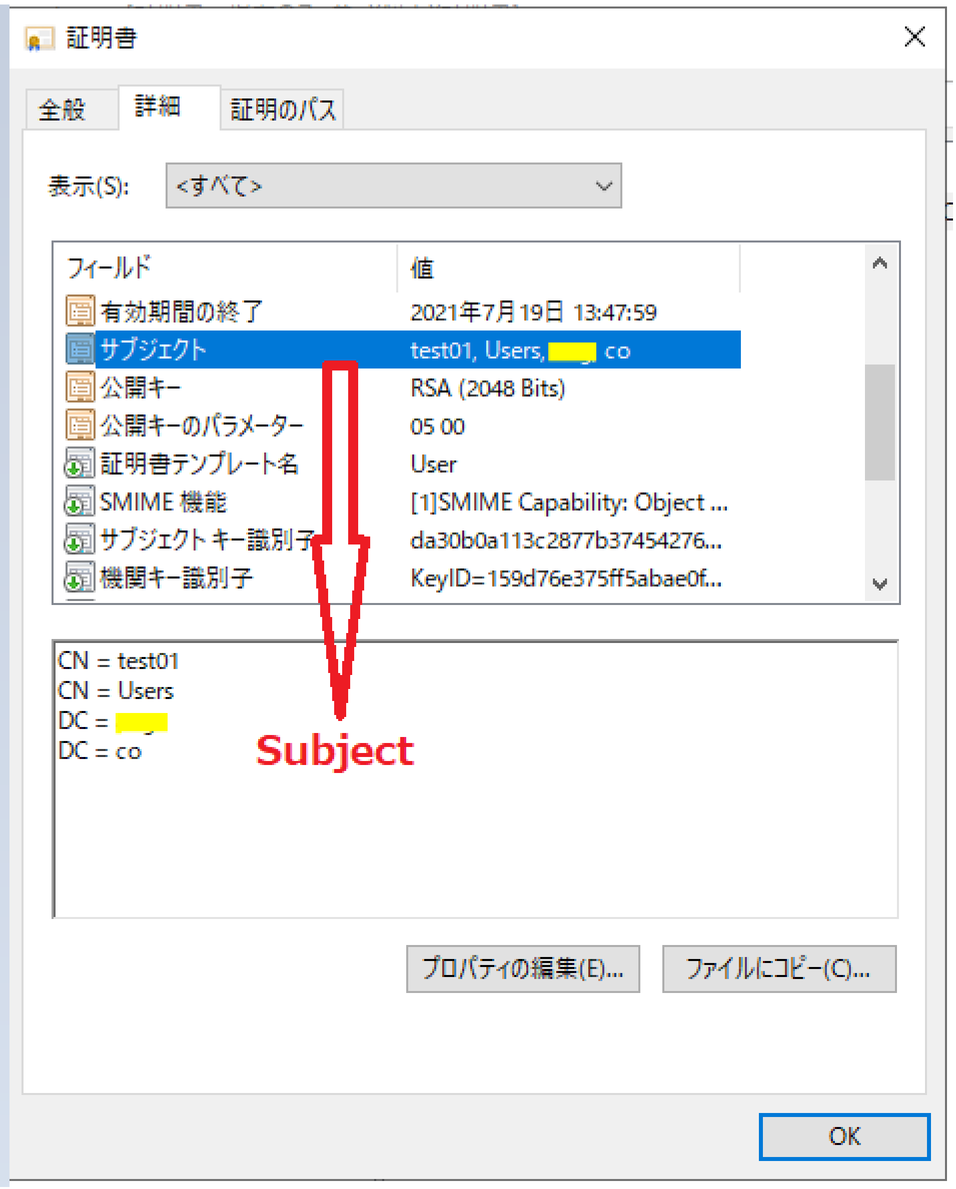
Smart card required for interactive

アカウントの期限

● なし(V)

○ 有効期限(E): 2020年 8月18日

Setting requires logon with smart card.

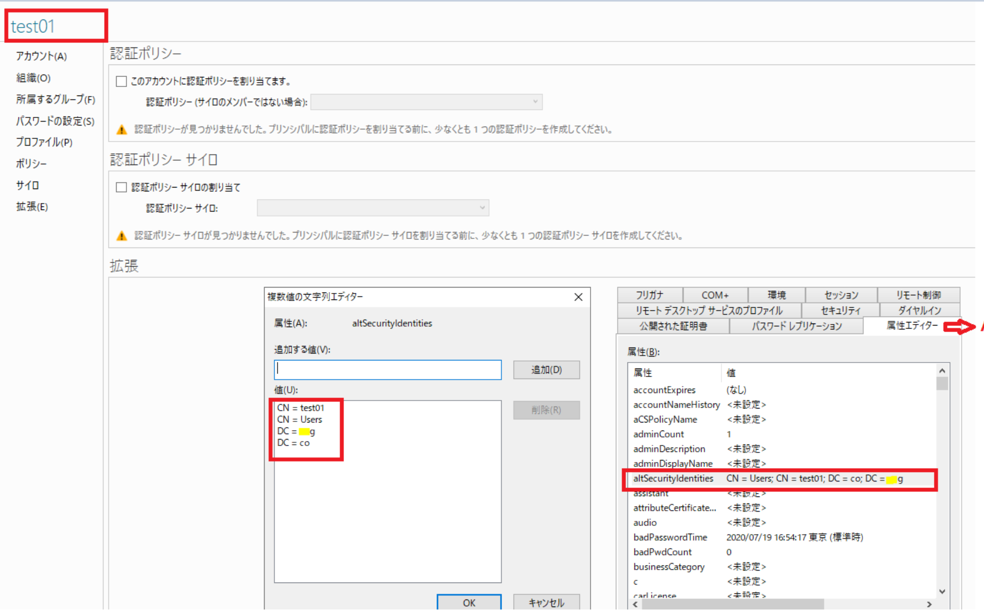


表示(S): <すべて>

フィールド	値
有効期間の終了	2021年7月19日 13:47:59
サブジェクト	test01, Users, [redacted] co
公開キー	RSA (2048 Bits)
公開キーのパラメーター	05 00
証明書テンプレート名	User
SMIME 機能	[1]SMIME Capability: Object ...
サブジェクト キー識別子	da30b0a113c2877b37454276...
機関キー識別子	KeyID=159d76e375ff5abae0f...

```
CN = test01
CN = Users
DC = [redacted]
DC = co
```

Get subject to mapping with username (See next the below image)



□ このアカウントに認証ポリシーを割り当てます。

認証ポリシー (サイロのメンバーではない場合):

認証ポリシーが見つかりませんでした。プリンシパルに認証ポリシーを割り当てる前に、少なくとも 1 つの認証ポリシーを作成してください。

□ 認証ポリシー サイロの割り当て

認証ポリシー サイロ:

認証ポリシー サイロが見つかりませんでした。プリンシパルに認証ポリシー サイロを割り当てる前に、少なくとも 1 つの認証ポリシー サイロを作成してください。

複数値の文字列エディター

属性(A): altSecurityIdentities

追加する値(V):

値(U):

CN = test01
CN = Users
DC = [redacted]g
DC = co

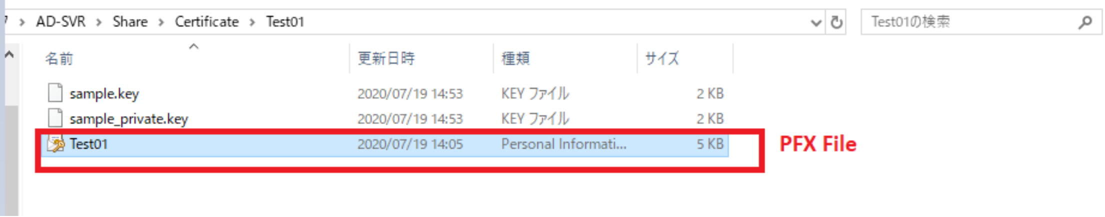
属性(B):

属性	値
accountExpires	(なし)
accountNameHistory	<未設定>
aCSPolicyName	<未設定>
adminCount	1
adminDescription	<未設定>
adminDisplayName	<未設定>
altSecurityIdentities	CN = Users; CN = test01; DC = co; DC = [redacted]g
assistant	<未設定>
attributeCertificate...	<未設定>
audio	<未設定>
badPasswordTime	2020/07/19 16:54:17 東京 (標準時)
badPwdCount	0
businessCategory	<未設定>
c	<未設定>
carLicense	<未設定>

Attribute editor

mapping the subject with username

Next, Export the certificate to the pfx format (including the private key) for use by the client.



名前	更新日時	種類	サイズ
sample.key	2020/07/19 14:53	KEY ファイル	2 KB
sample_private.key	2020/07/19 14:53	KEY ファイル	2 KB
Test01	2020/07/19 14:05	Personal Informati...	5 KB

PFX File

2. Client Side

- Window Setting:

  2.1.[ComputerConfiguration]->[AdministrativeTemplates]->[WindowsComponents]->[Smart Cards]

  -Enable "Allow certificates without extended key usage certificate attribute".

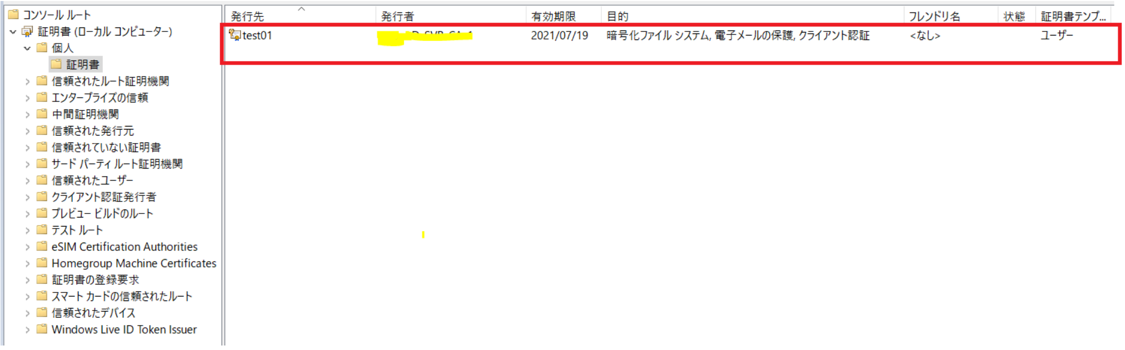
  - Enable "Allow signing keys to be used for logon".

  - Enable "Force reading of all certificates from smart card".

  2.2. [Computer Configuration]-> [Administrative Templates]->[System]->[Logon]

  - Enable "Always wait for network at computer startup and logon".

- import PFX file for KSP to read and sign the certificate.:



発行先	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプ...
test01	[redacted]	2021/07/19	暗号化ファイル システム, 電子メールの保護, クライアント認証	<なし>		ユーザー